doi: 10.11845/sxjz.2016018b

Error-correcting Codes Based on Totally Isotropic Subspaces in Symplectic Spaces

GUO Jun[1,*], LI Fenggao[2]

(*1. College of Mathematics and Information Science, Langfang Teachers University, Langfang, Hebei, 065000, P. R. China; 2. College of Mathematics, Hunan Institute of Science and Technology, Yueyang, Hunan, 414006, P. R. China*)

Abstract: Let $\mathbb{F}_q^{2\nu}$ be the 2ν-dimensional symplectic space over the field $\mathbb{F}_q$ with q elements. For $0 \leq m \leq \nu$, let $\mathcal{M}(m,0;2\nu)$ denote the set of all m-dimensional totally isotropic subspaces of $\mathbb{F}_q^{2\nu}$ and $\mathcal{M}(2\nu)=\bigcup_{m=0}^{\nu}\mathcal{M}(m,0;2\nu)$. In this paper, we present several bounds on the size of codes in $\mathcal{M}(2\nu)$, and prove that the codes in $\mathcal{M}(m,0;2\nu)$ achieve the Wang-Xing-Safavi-Naini bound if and only if they are certain Steiner structures.

Keywords: error-correcting code; symplectic space; totally isotropic subspace; Steiner structure

MR(2010) Subject Classification: 94B65; 51E10; 94B25 / **CLC number:** O157.4
Document code: A **Article ID:** 1000-0917(2017)06-0919-13

0 Introduction

Let $\mathbb{F}_q^n$ be the n-dimensional row vector space over the field $\mathbb{F}_q$ with q elements. The projective space of order n over $\mathbb{F}_q$, denoted by $\mathcal{P}_q(n)$, is the set of all subspaces of $\mathbb{F}_q^n$. The natural measure of distance in $\mathcal{P}_q(n)$ is given by

$$d(U,W)=\dim U+\dim W-2\dim(U\cap W) \tag{1}$$

for $U,W\in\mathcal{P}_q(n)$. Then $\mathcal{P}_q(n)$ is a metric space. A *code* $\mathbb{C}$ is a nonempty subset of $\mathcal{P}_q(n)$. The *minimum distance* between distinct codewords in a code $\mathbb{C}$ is denoted by $d(\mathbb{C})$, i.e. $d(\mathbb{C})=\min_{U,W\in\mathbb{C},U\neq W} d(U,W)$. Codes in the projective space have several applications, such as noncoherent linear network coding[9] and linear authentication[15]. Kötter and Kschischang[9] showed that a code with minimum distance $d>2t+2\rho$ can correct any t packet errors and any ρ packet erasures introduced (adversarially) anywhere in the network. Coding in the projective space has received recently a lot of attention due to its application in network coding.

The determination of bounds on the size of codes with given minimum distance is the main problem in the context of coding theory. Bounds on the size of codes in the projective space are considered in recent years: see [9] for the Sphere-packing bound and Singleton bound, [15] for the Wang-Xing-Safavi-Naini bound, [4] for the anticode bound, Johnson bound and Gilbert-Varshamov bound and [1] for the Ahlswede-Aydinian Bound. Xia et al.[16] studied the relations of bounds on the size of codes and Steiner structures. Gao and Wang[5] studied some subcodes of

Received date: 2016-01-27. Revised date: 2016-06-27.
Foundation item: This work is supported by NSF of Hebei Province (No. A2016408016), NSFC (No. 11271047) and the Fund for Hundreds of Excellent Innovative Talents in Higher Education of Hebei Province (No. BR2-235).

E-mail: * guojun_lf@163.com

codes in the projective space, and provided analogs of the above results in the attenuated space. In this paper, we continue to study other subcodes of codes in the projective space, and provide analogs of these results in the symplectic space.

Let $\mathbb{F}_q^{2\nu}$ be the 2ν-dimensional symplectic space, and let $\mathcal{M}(m,0;2\nu)$ denote the set of all m-dimensional totally isotropic subspaces of $\mathbb{F}_q^{2\nu}$ (see Section 1). Suppose that $\mathcal{M}(2\nu)=\bigcup_{m=0}^{\nu}\mathcal{M}(m,0;2\nu)$. We say that $\mathbb{C}\subseteq\mathcal{M}(2\nu)$ is a $(2\nu,M,d)$ *code* in $\mathcal{M}(2\nu)$ if $|\mathbb{C}|=M$ and $d(U,W)\geq d$ for all U,W in $\mathbb{C}$. If a $(2\nu,M,d)$ code $\mathbb{C}$ is contained in $\mathcal{M}(m,0;2\nu)$ for some m, $\mathbb{C}$ is called a $(2\nu,M,d,m)$ code. Let $\mathcal{A}(2\nu,d,m)$ denote the maximum number of codewords in a $(2\nu,M,d,m)$ code in $\mathcal{M}(m,0;2\nu)$. A $(2\nu,M,d,m)$ code in $\mathcal{M}(m,0;2\nu)$ is called *optimal* if it has $\mathcal{A}(2\nu,d,m)$ codewords. For general theory of error-correcting codes, the readers may consult [8, 10].

In this paper, we study the error-correcting codes in $\mathcal{M}(2\nu)$. This paper is structured as follows. In Section 1, we introduce the concept of the symplectic space and some useful lemmas. In Section 2, we discuss the Sphere-packing bound and Wang-Xing-Safavi-Naini bound on the size of codes in $\mathcal{M}(m;2\nu)$. In Section 3, we discuss the anticode bound and Ahlswede-Aydinian bound on the size of codes in $\mathcal{M}(m;2\nu)$. In Section 4, we discuss the Johnson bound and Gilbert-Varshamov bound on the size of codes in $\mathcal{M}(m;2\nu)$. In Section 5, we introduce Steiner structures in the symplectic space and prove that the codes in $\mathcal{M}(m,0;2\nu)$ achieve the Wang-Xing-Safavi-Naini bound if and only if they are certain Steiner structures. In Section 6, we discuss the upper and lower bounds on the size of codes in $\mathcal{M}(2\nu)$.

1 Symplectic Space

Let K be a $2\nu\times 2\nu$ nonsingular alternate matrix over $\mathbb{F}_q$. A $2\nu\times 2\nu$ matrix T over $\mathbb{F}_q$ is called a *symplectic matrix* with respect to K if $TKT^{\mathrm{t}}=K$, where T^{t} is the transpose of T. The *symplectic group* of degree 2ν with respect to K over $\mathbb{F}_q$, denoted by $\mathrm{Sp}_{2\nu}(\mathbb{F}_q,K)$, consists of all $2\nu\times 2\nu$ symplectic matrices with respect to K over $\mathbb{F}_q$. Let K and K' be two $2\nu\times 2\nu$ nonsingular alternate matrices over $\mathbb{F}_q$. Then there is a $2\nu\times 2\nu$ nonsingular matrix Q over $\mathbb{F}_q$ such that $QKQ^{\mathrm{t}}=K'$, which implies that $T\in\mathrm{Sp}_{2\nu}(\mathbb{F}_q,K)$ if and only if $QTQ^{-1}\in\mathrm{Sp}_{2\nu}(\mathbb{F}_q,K')$, and therefore $\mathrm{Sp}_{2\nu}(\mathbb{F}_q,K)$ is isomorphic to $\mathrm{Sp}_{2\nu}(\mathbb{F}_q,K')$. Thus, in discussing symplectic groups, we can choose any particular $2\nu\times 2\nu$ nonsingular alternate matrix K and study $\mathrm{Sp}_{2\nu}(\mathbb{F}_q,K)$.

From now on let us take

$$K=\begin{pmatrix}0 & I^{(\nu)}\\ -I^{(\nu)} & 0\end{pmatrix},$$

denote the symplectic group with respect to K over $\mathbb{F}_q$ simply by $\mathrm{Sp}_{2\nu}(\mathbb{F}_q)$, and call it the *symplectic group* of degree 2ν over $\mathbb{F}_q$. There is a right multiplication action of $\mathrm{Sp}_{2\nu}(\mathbb{F}_q)$ on $\mathbb{F}_q^{2\nu}$ defined as follows:

$$\begin{aligned}&\mathbb{F}_q^{2\nu}\times\mathrm{Sp}_{2\nu}(\mathbb{F}_q)\to\mathbb{F}_q^{2\nu}\\ &((x_1,x_2,\cdots,x_{2\nu}),T)\mapsto(x_1,x_2,\cdots,x_{2\nu})T.\end{aligned}$$

The vector space $\mathbb{F}_q^{2\nu}$ together with the right multiplication action of $\mathrm{Sp}_{2\nu}(\mathbb{F}_q)$ is called the 2ν-dimensional *symplectic space* over $\mathbb{F}_q$.

For an m-dimensional subspace P in $\mathbb{F}_q^{2\nu}$, we mean by a matrix representation of P an $m\times 2\nu$ matrix whose rows form a basis of P, denoted by the same symbol P. An m-dimensional subspace P in the 2ν-dimensional symplectic space is said to be of *type* (m,s), if PKP^{t} is of rank $2s$. In particular, subspaces of type $(m,0)$ are called m-dimensional *totally isotropic subspaces*. Denote by $\mathcal{M}(m,s;2\nu)$ the set of all subspaces of type (m,s) of $\mathbb{F}_q^{2\nu}$ and by $N(m,s;2\nu)$ the size of the set $\mathcal{M}(m,s;2\nu)$. By Theorem 3.7 in [14], each set $\mathcal{M}(m,s;2\nu)$ forms an orbit under $\mathrm{Sp}_{2\nu}(\mathbb{F}_q)$. Let P be an m-dimensional subspace of $\mathbb{F}_q^{2\nu}$. Then $P^{\perp}=\{y\in\mathbb{F}_q^{2\nu}\mid yKx^{\mathrm{t}}=0 \text{ for all } x\in P\}$ is called the *dual subspace* of P. Notation and terminology are adopted from Wan's book [14].

Now we introduce some useful lemmas, which are included for later reference.

Lemma 1.1[14, Corollary 3.19] Let $1\le m\le\nu$. Then

$$N(m,0;2\nu)=\begin{bmatrix}\nu\\ m\end{bmatrix}_q\prod_{t=\nu-m+1}^{\nu}(q^t+1).$$

Lemma 1.2[14, Corollary 3.20] Let $1\le s\le\nu$. Then

$$N(2s,s;2\nu)=q^{2s(\nu-s)}\begin{bmatrix}\nu\\ s\end{bmatrix}_q\prod_{t=\nu-s+1}^{\nu}(q^t+1)\Big/\prod_{t=1}^{s}(q^t+1).$$

Given a subspace P of type (m,s) in $\mathbb{F}_q^{2\nu}$, let $\mathcal{M}(i;m,s;m_1,s_1;2\nu)$ be the set of all subspaces U of type (m_1,s_1) satisfying $\dim(P\cap U)=i$. By the transitivity of $Sp_{2\nu}(\mathbb{F}_q)$ on the set of subspaces of type (m,s), the size of $\mathcal{M}(i;m,s;m_1,s_1;2\nu)$, denoted by $N(i;m,s;m_1,s_1;2\nu)$, is independent of the particular choice of the subspace P of type (m,s).

Lemma 1.3[6, Theorem 2.5] Let $\max\{0,2s+m-2\nu\}\le i\le s\le\nu$ and $i\le m\le\nu$. Then

$$\begin{aligned}N(i;m,0;2s,s;2\nu)=&\sum_{\rho=\max\{s-i,2s-2i-\nu+m\}}^{\min\{2s-2i,\nu-i\}}q^{(2\nu-2s)(2s-i-\rho)+(\rho-s+i)(2\nu+\rho-3s+i)}\\&\times\prod_{t=1}^{\rho-s+i}(q^{2t-1}-1)\begin{bmatrix}\nu-2s+i+\rho\\ 2\rho-2s+2i\end{bmatrix}_q\begin{bmatrix}\nu-m\\ 2s-2i-\rho\end{bmatrix}_q\begin{bmatrix}m\\ i\end{bmatrix}_q.\end{aligned}$$

Lemma 1.4[6, Corollary 2.6] Let $\max\{0,2s+m-2\nu\}\le i\le s\le\nu$ and $i\le m\le\nu$. Then

$$N(i;2s,s;m,0;2\nu)=\frac{N(i;m,0;2s,s;2\nu)N(m,0;2\nu)}{N(2s,s;2\nu)},$$

where $N(m,0;2\nu),N(2s,s;2\nu)$ and $N(i;m,0;2s,s;2\nu)$ are given by Lemmas 1.1, 1.2 and 1.3, respectively.

Lemma 1.5[6, Theorem 2.10] Let $0\le i\le s$ and $i\le m\le\nu$. Then

$$\begin{aligned}N(i;m,0;s,0;2\nu)=&\sum_{j=\max\{0,m+s-\nu-i\}}^{s-i}\ \sum_{t=\max\{0,m+s-\nu-i\}}^{\min\{j,m-i\}}q^{\omega}\\&\times\begin{bmatrix}m-i\\ t\end{bmatrix}_q\begin{bmatrix}\nu-m\\ j-t\end{bmatrix}_q\begin{bmatrix}\nu+t-m-j\\ s-i-j\end{bmatrix}_q\begin{bmatrix}m\\ i\end{bmatrix}_q,\end{aligned}$$

where $\omega=\frac{t(t+1)}{2}+\frac{(j-t)(j-t+1)}{2}+t(\nu-m)+j(\nu-m+t-s+i)+(s-i)(m-i-t)$.

2 Sphere-packing Bound and Wang-Xing-Safavi-Naini Bound

Since the distance between any two elements of $\mathcal{M}(m,0;2\nu)$ is always even, we only need to consider $\mathcal{A}(2\nu,d,m)$ for even $d=2j$.

The *sphere* of radius $2t$ centered at a subspace U in $\mathcal{M}(m,0;2\nu)$ is defined to be the set of all subspaces whose distance from U is less than or equal to $2t$, i.e., the set

$$S_{2t,m}(U)=\{W\in\mathcal{M}(m,0;2\nu)\mid d(U,W)\le 2t\}.$$

By (1) one obtains that

$$S_{2t,m}(U)=\{W\in\mathcal{M}(m,0;2\nu)\mid \dim(U\cap W)\ge m-t\}.$$

From Lemma 1.5 we deduce that

$$|S_{2t,m}(U)|=\sum_{i=0}^{t}N(m-i;m,0;m,0;2\nu). \tag{2}$$

Theorem 2.1 (Sphere-packing bound) Let $t=\lfloor\frac{j-1}{2}\rfloor$. Then

$$\mathcal{A}(2\nu,2j,m)\le\frac{\begin{bmatrix}\nu\\ m\end{bmatrix}_q\prod_{i=\nu-m+1}^{\nu}(q^i+1)}{\sum_{i=0}^{t}N(m-i;m,0;m,0;2\nu)}.$$

Proof Let $\mathbb{C}\subseteq\mathcal{M}(m,0;2\nu)$ be a $(2\nu,M,d,m)$ code. Then the spheres of radius $2t$ about distinct codewords in $\mathbb{C}$ are disjoint. By (2) each of these spheres contains

$$\sum_{i=0}^{t}N(m-i;m,0;m,0;2\nu)$$

subspaces in $\mathcal{M}(m,0;2\nu)$. Since $M\sum_{i=0}^{t}N(m-i;m,0;m,0;2\nu)$ cannot exceed the total number of subspaces in $\mathcal{M}(m,0;2\nu)$, which implies that $M\sum_{i=0}^{t}N(m-i;m,0;m,0;2\nu)\le N(m,0;2\nu)$. By Lemma 1.1, the desired result follows. □

Wang et al.[15] provided the bound on the size of codes in the projective space, which is called the Wang-Xing-Safavi-Naini bound. The following theorem is an analog of this bound in the symplectic space.

Theorem 2.2 (Wang-Xing-Safavi-Naini bound) Let $j\le m$. Then

$$\mathcal{A}(2\nu,2j,m)\le\prod_{t=0}^{m-j}\frac{q^{2(\nu-t)}-1}{q^{m-t}-1}:=B_{\mathrm{WXS}}.$$

Proof Let $\mathbb{C}\subseteq\mathcal{M}(m,0;2\nu)$ be a $(2\nu,M,2j,m)$ code. Then each codeword of $\mathbb{C}$ contains exactly $\begin{bmatrix}m\\ m-j+1\end{bmatrix}_q$ many $(m-j+1)$-dimensional totally isotropic subspaces. On the other hand, any given $(m-j+1)$-dimensional totally isotropic subspace of $\mathbb{F}_q^{2\nu}$ cannot be contained in two distinct codewords of $\mathbb{C}$. In fact, suppose that U and W are two distinct codewords of $\mathbb{C}$ with $\dim(U\cap W)\ge m-j+1$. By (1) we have that

$$d(U,W)=2m-2\dim(U\cap W)\le 2m-2(m-j+1)=2(j-1),$$

a contradiction. Therefore, $M\genfrac{[}{]}{0pt}{}{m}{m-j+1}_q$ cannot exceed the total number of subspaces in $\mathcal{M}(m-j+1,0;2\nu)$, which implies that $M\genfrac{[}{]}{0pt}{}{m}{m-j+1}_q \le N(m-j+1,0;2\nu)$. From Lemma 1.1 we deduce that

$$M \le \frac{N(m-j+1,0;2\nu)}{\genfrac{[}{]}{0pt}{}{m}{m-j+1}_q} = \frac{\prod_{t=\nu-m+j}^{\nu}(q^{2t}-1)}{\prod_{t=j}^{m}(q^t-1)} = \prod_{t=0}^{m-j}\frac{q^{2(\nu-t)}-1}{q^{m-t}-1},$$

as desired. □

3 Anticode Bound and Ahlswede-Aydinian Bound

An *anticode* $\mathbb{A}(2t)$ of diameter $2t$ in $\mathcal{M}(m,0;2\nu)$ is any subset of $\mathcal{M}(m,0;2\nu)$ such that $d(U,W) \le 2t$ for all $U,W \in \mathbb{A}(2t)$. The optimal (largest) anticodes in $\mathcal{M}(m,0;2\nu)$ were found by the first author of this article, Ma and Wang[7].

Lemma 3.1[7] Assume that either $j=2$ and $q+1 < N(m,0;2\nu)/N(m-1,0;2\nu)$, or $j>2$ and $\genfrac{[}{]}{0pt}{}{m}{m-j+1}_q < N(m,0;2\nu)/N(m-j+1,0;2\nu)$. Then the size of the largest anticode of diameter $2(j-1)$ in $\mathcal{M}(m,0;2\nu)$ is $\genfrac{[}{]}{0pt}{}{m}{m-j+1}_q N(m,0;2\nu)/N(m-j+1,0;2\nu)$.

In [1], Ahlswede and Aydinian obtained a useful result based on vertex transitive graphs.

Lemma 3.2[1, Lemma 1] Let $\Gamma=(V,E)$ be a graph that admits a transitive group of automorphisms $\mathrm{Aut}(\Gamma)$ and let A,B be arbitrary subsets of the vertex set V. Then there exists some $g \in \mathrm{Aut}(\Gamma)$ such that

$$\frac{|g(A)\cap B|}{|B|} \ge \frac{|A|}{|V|}.$$

By using Lemma 3.2 we obtain the following result.

Lemma 3.3 Let $\mathbb{C} \subseteq \mathcal{M}(m,0;2\nu)$ be a $(2\nu,M,2j,m)$ code. Then for an arbitrary subset $\mathcal{B} \subseteq \mathcal{M}(m,0;2\nu)$, there exists a $(2\nu,M^*,2j,m)$ code $\mathbb{C}^* \subseteq \mathcal{B}$ such that

$$\frac{M^*}{|\mathcal{B}|} \ge \frac{M}{N(m,0;2\nu)}.$$

Proof Define a graph Γ with the vertex set $\mathcal{M}(m,0;2\nu)$, and two vertices P and Q are adjacent if $\dim(P\cap Q)=m-1$. Then Γ admits a transitive group of automorphisms $\mathit{Sp}_{2\nu}(\mathbb{F}_q)$. By Lemma 3.2 there exists some $T \in \mathrm{Sp}_{2\nu}(\mathbb{F}_q)$ such that

$$\frac{|\{UT \mid U \in \mathbb{C}\}\cap\mathcal{B}|}{|\mathcal{B}|} \ge \frac{M}{N(m,0;2\nu)}.$$

Let $\mathbb{C}^* = \{UT \mid U \in \mathbb{C}\}\cap\mathcal{B}$. For any $U,W \in \mathbb{C}^*$, there exist $U_1,W_1 \in \mathbb{C}$ such that $U_1T=U$ and $W_1T=W$, which imply that $\dim(U\cap W)=\dim(U_1T\cap W_1T)=\dim(U_1\cap W_1)T=\dim(U_1\cap W_1)$. It follows that $\mathbb{C}^* \subseteq \mathcal{B}$ is a $(2\nu,M^*,2j,m)$ code with $M^*=|\{UT \mid U \in \mathbb{C}\}\cap\mathcal{B}|$. Therefore, the desired result follows. □

By Lemmas 3.1 and 3.3, we immediately obtain the following bound, which is an analog of the anticode bound in the projective space.

Theorem 3.1 (Anticode bound) Assume that either $j=2$ and $q+1 < N(m,0;2\nu)/N(m-1,0;2\nu)$, or $j>2$ and $\genfrac{[}{]}{0pt}{}{m}{m-j+1}_q < N(m,0;2\nu)/N(m-j+1,0;2\nu)$. Then

$$\mathcal{A}(2\nu,2j,m) \le B_{\mathrm{WXS}}.$$

Proof Let $\mathbb{C}$ be a $(2\nu, M, 2j, m)$ code and $\mathbb{A}(2(j-1))$ be the largest anticodes in $\mathcal{M}(m, 0; 2\nu)$. Then $\mathbb{C} \cap \mathbb{A}(2(j-1))$ has at most one element. By Lemmas 1.1, 3.1 and 3.3 we have

$$\begin{aligned}\mathcal{A}(2\nu, 2j, m) &\leq \frac{N(m,0;2\nu)}{|\mathbb{A}(2(j-1))|} = \frac{N(m-j+1,0;2\nu)}{\left[{m \atop m-j+1}\right]_q} \\ &= \frac{\prod_{t=\nu-m+j}^{\nu}(q^{2t}-1)}{\prod_{t=j}^{m}(q^t-1)} = \prod_{t=0}^{m-j}\frac{q^{2(\nu-t)}-1}{q^{m-t}-1} = B_{\text{WXS}}\end{aligned}$$

as desired. □

Ahlswede and Aydinian[1] provided the bound on the size of codes in the projective space, which is called the Ahlswede-Aydinian bound. The following theorem is an analog of this bound in the symplectic space.

Theorem 3.2 (Ahlswede-Aydinian bound) For integers $0 \leq i < j \leq m$ and $m-i \leq r \leq \nu$, we have

$$\mathcal{A}(2\nu, 2j, m) \leq \frac{N(m,0;2\nu)\mathcal{A}(2r, 2(j-i), m-i)}{\sum_{t=m-i}^{r} N(t; 2r, r; m, 0; 2\nu)}.$$

Proof Let $\mathbb{C} \subseteq \mathcal{M}(m, 0; 2\nu)$ be a $(2\nu, M, d, m)$ code. Let V be a fixed subspace of type $(2r, r)$ in $\mathbb{F}_q^{2\nu}$. Define

$$\mathcal{B} = \{U \in \mathcal{M}(m, 0; 2\nu) \mid \dim(U \cap V) \geq m - i\}.$$

By Lemma 1.4 the size of $\mathcal{B}$ is

$$\sum_{t=m-i}^{r} N(t; 2r, r; m, 0; 2\nu).$$

By Lemma 3.3 there exists a $(2\nu, M^*, 2j, m)$ code $\mathbb{C}^* \subseteq \mathcal{B}$ such that

$$M \leq \frac{M^* N(m, 0; 2\nu)}{|\mathcal{B}|}.$$

Define

$$\mathbb{C}_1 = \{U_1 = \mathcal{H}_{m-i}(U \cap V) \mid U \in \mathbb{C}^*\},$$

where $\mathcal{H}_{m-i}(U \cap V) = U \cap V$ if $\dim(U \cap V) = m - i$; otherwise $\mathcal{H}_{m-i}(U \cap V)$ is some $(m-i)$-dimensional subspace of $U \cap V$. Let U and W be any two distinct codewords of code $\mathbb{C}^*$. Then $d(U, W) = 2m - 2\dim(U \cap W) \geq 2j$, which implies that $\dim(U \cap W) \leq m - j$. For $U_1 = \mathcal{H}_{m-i}(U \cap V)$ and $W_1 = \mathcal{H}_{m-i}(W \cap V)$, we have

$$\begin{aligned}d(U_1, W_1) &= 2(m-i) - 2\dim(U_1 \cap W_1) \geq 2(m-i) - 2\dim(U \cap W) \\ &\geq 2(m-i) - 2(m-j) = 2(j-i) \geq 2,\end{aligned}$$

which implies that U_1 and W_1 are distinct. Therefore, both $\mathbb{C}^*$ and $\mathbb{C}_1$ have the same size, and $\mathbb{C}_1$ is a $(2r, M^*, 2(j-i), m-i)$ code. From $M^* \leq \mathcal{A}(2r, 2(j-i), m-i)$ we deduce that

$$M \leq \frac{N(m,0;2\nu)\mathcal{A}(2r, 2(j-i), m-i)}{|\mathcal{B}|}$$

as desired. □

4 Johnson Bound and Gilbert-Varshamov Bound

In this section, we obtain the two Johnson bounds and Gilbert-Varshamov bound on the size of codes in the symplectic space, which are analogs of these bounds in the projective space.

Let e_i be the 2ν-dimensional row vector whose ith component is 1 and other components are 0. For $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{F}_q^{2\nu}$, let $\langle \alpha_1, \alpha_2, \cdots, \alpha_n \rangle$ denote the subspace generated by $\alpha_1, \alpha_2, \cdots, \alpha_n$.

Theorem 4.1 (Johnson bound I) Let $j \leq m-1$. Then

$$\mathcal{A}(2\nu, 2j, m) \leq \frac{q^{2\nu}-1}{q^m-1}\mathcal{A}(2(\nu-1), 2j, m-1).$$

Proof Let $\mathbb{C} \subseteq \mathcal{M}(m, 0; 2\nu)$ be a $(2\nu, M, 2j, m)$ code. Then each codeword of $\mathbb{C}$ contains exactly $\begin{bmatrix} m \\ 1 \end{bmatrix}_q$ many one-dimensional subspaces. Since the total number of one-dimensional subspaces is $\frac{q^{2\nu}-1}{q-1}$, there is a one-dimensional subspace that is contained in at least $M\frac{q^m-1}{q^{2\nu}-1}$ codewords of $\mathbb{C}$.

Pick a fixed one-dimensional subspace $\langle e_1 \rangle$. Then $\langle e_1 \rangle^\perp = \langle e_1, e_2, \cdots, e_\nu, e_{\nu+2}, \cdots, e_{2\nu} \rangle$. For $U \in \mathcal{M}(m, 0; 2\nu)$, if $e_1 \in U$ then $U \subseteq \langle e_1 \rangle^\perp$ and therefore $U \cap \langle e_2, \cdots, e_\nu, e_{\nu+2}, \cdots, e_{2\nu} \rangle$ is of dimension $m-1$. Define

$$\mathbb{C}' = \{U \cap \langle e_2, \cdots, e_\nu, e_{\nu+2}, \cdots, e_{2\nu} \rangle \mid U \in \mathbb{C}, e_1 \in U\}.$$

Since $\langle e_2, \cdots, e_\nu, e_{\nu+2}, \cdots, e_{2\nu} \rangle$ is isomorphic to $\mathbb{F}_q^{2(\nu-1)}$, without loss of generality, let $\mathbb{C}'$ be a $(2(\nu-1), M', 2j', m-1)$ code with $M' \geq M\frac{q^m-1}{q^{2\nu}-1}$.

Now we show that $j = j'$. Let U' and W' be any two codewords of $\mathbb{C}'$. Then there exist $U, W \in \mathbb{C}$ such that $U' = U \cap \langle e_2, \cdots, e_\nu, e_{\nu+2}, \cdots, e_{2\nu} \rangle$ and $W' = W \cap \langle e_2, \cdots, e_\nu, e_{\nu+2}, \cdots, e_{2\nu} \rangle$. By $e_1 \in U \cap W$ we have $U \cap W \subseteq \langle e_1 \rangle^\perp$, which implies that

$$\langle e_1 \rangle^\perp = (U \cap W) + \langle e_2, \cdots, e_\nu, e_{\nu+2}, \cdots, e_{2\nu} \rangle.$$

Therefore, one obtains that

$$\begin{aligned} \dim(U' \cap W') &= \dim(U \cap W \cap \langle e_2, \cdots, e_\nu, e_{\nu+2}, \cdots, e_{2\nu} \rangle) \\ &= \dim(U \cap W) + 2(\nu-1) - \dim((U \cap W) + \langle e_2, \cdots, e_\nu, e_{\nu+2}, \cdots, e_{2\nu} \rangle) \\ &= \dim(U \cap W) - 1. \end{aligned}$$

By (1) we have $j = j'$, and therefore

$$\mathcal{A}(2(\nu-1), 2j, m-1) \geq M' \geq M\frac{q^m-1}{q^{2\nu}-1}$$

as desired. □

Applying Theorem 4.1 iteratively $m-j+1$ times, stopping with the trivial equality $\mathcal{A}(2(\nu-m+j-1), 2j, j-1) = 1$, we obtain the following result.

Corollary 4.1

$$\mathcal{A}(2\nu, 2j, m) \leq B_{\mathrm{WXS}}.$$

Theorem 4.2 (Johnson bound II) Let $j \leq m \leq \nu - 1$. Then

$$\mathcal{A}(2\nu, 2j, m) \leq \frac{q^{2\nu} - 1}{q^{2(\nu-m)} - 1}\mathcal{A}(2(\nu-1), 2j, m).$$

Proof Let $\mathbb{C} \subseteq \mathcal{M}(m, 0; 2\nu)$ be a $(2\nu, M, 2j, m)$ code. For each subspace V of type $(2(\nu-1), \nu-1)$ of $\mathbb{F}_q^{2\nu}$, define

$$\mathbb{C}_V = \{U \in \mathbb{C} \mid U \subseteq V\}.$$

Then $\mathbb{C}_V$ is a $(2(\nu-1), M_V, 2j', m)$ code with $j' \geq j$. For any given m-dimensional totally isotropic subspace P of $\mathbb{F}_q^{2\nu}$, by Lemma 1.3 there are $N(m; m, 0; 2(\nu-1), \nu-1; 2\nu)$ many subspaces of type $(2(\nu-1), \nu-1)$ of $\mathbb{F}_q^{2\nu}$ containing P. It follows that each codeword of $\mathbb{C}$ belongs to $N(m; m, 0; 2(\nu-1), \nu-1; 2\nu)$ distinct codes $\mathbb{C}_V$, and therefore

$$\sum_{V \in \mathcal{M}(2(\nu-1), \nu-1; 2\nu)} |\mathbb{C}_V| = MN(m; m, 0; 2(\nu-1), \nu-1; 2\nu).$$

Hence, there exists at least one V of type $(2(\nu-1), \nu-1)$ such that $|\mathbb{C}_V| \geq MN(m; m, 0; 2(\nu-1), \nu-1; 2\nu)/N(2(\nu-1), \nu-1; 2\nu)$. Since $\mathcal{A}(2(\nu-1), 2j, m) \geq |\mathbb{C}_V|$, we have

$$\begin{aligned}\mathcal{A}(2\nu, 2j, m) &\leq \frac{N(2(\nu-1), \nu-1; 2\nu)\mathcal{A}(2(\nu-1), 2j, m)}{N(m; m, 0; 2(\nu-1), \nu-1; 2\nu)} \\ &= \frac{q^{2\nu} - 1}{q^{2(\nu-m)} - 1}\mathcal{A}(2(\nu-1), 2j, m)\end{aligned}$$

as desired. □

Corollary 4.2 Let $j \leq m \leq \nu - 1$. Then

$$\mathcal{A}(2\nu, 2j, m) \leq \prod_{t=0}^{m-j}(q^{m-t} + 1) \prod_{t=0}^{\nu-m-1} \frac{q^{2(\nu-t)} - 1}{q^{2(\nu-t-m)} - 1}.$$

Proof From Theorems 4.2 and 2.2 we deduce that

$$\begin{aligned}\mathcal{A}(2\nu, 2j, m) &\leq \mathcal{A}(2m, 2j, m) \prod_{t=0}^{\nu-m-1} \frac{q^{2(\nu-t)} - 1}{q^{2(\nu-t-m)} - 1} \\ &\leq \prod_{t=0}^{m-j}(q^{m-t} + 1) \prod_{t=0}^{\nu-m-1} \frac{q^{2(\nu-t)} - 1}{q^{2(\nu-t-m)} - 1}\end{aligned}$$

as desired. □

Theorem 4.3 (Gilbert-Varshamov bound) Let $j \leq m$. Then

$$\mathcal{A}(2\nu, 2j, m) \geq \frac{\begin{bmatrix}\nu \\ m\end{bmatrix}_q \prod_{t=\nu-m+1}^{\nu}(q^t + 1)}{\sum_{i=0}^{j-1} N(m-i; m, 0; m, 0; 2\nu)}.$$

Proof Let $\mathbb{C} \subseteq \mathcal{M}(m, 0; 2\nu)$ be a $(2\nu, M, 2j, m)$ code. Then there is no subspace U in $\mathcal{M}(m, 0; 2\nu)$ such that $d(U, W) \geq 2j$ for all $W \in \mathbb{C}$. Therefore, for any subspace U in $\mathcal{M}(m, 0; 2\nu)$, there exists a sphere of radius $2(j-1)$ centered at some $W \in \mathbb{C}$ such that $U \in S_{2(j-1),m}(W)$, which implies that

$$\sum_{W \in \mathbb{C}} |S_{2(j-1),m}(W)| \geq N(m, 0; 2\nu).$$

By the transitivity of $Sp_{2\nu}(\mathbb{F}_q)$ on the set of subspaces of the same type, we have

$$\sum_{W\in\mathbb{C}} |S_{2(j-1),m}(W)| = M|S_{2(j-1),m}(W)|,$$

and therefore $M \geq N(m,0;2\nu)|/|S_{2(j-1),m}(W)|$ as desired. □

Remark 4.1 Let $\nu = 2$. The bounds listed in Sections 2, 3 and 4 are given in the following table:

Name	$(j,m)=(1,2)$	$(j,m)=(1,1)$	$(j,m)=(2,2)$
Sphere-packing bound	$(q+1)(q^2+1)$	$(q+1)(q^2+1)$	$(q+1)(q^2+1)$
Wang-Xing-Safavi-Naini bound	$(q+1)(q^2+1)$	$(q+1)(q^2+1)$	q^2+1
Anticode bound			q^2+1
Johnson bound I	$(q+1)(q^2+1)$		
Johnson bound II		$(q+1)(q^2+1)$	
Gilbert-Varshamov bound	$(q+1)(q^2+1)$	$(q+1)(q^2+1)$	$\frac{(q+1)(q^2+1)}{q(q+1)+1}$

5 Steiner Structures

In [11], Schwartz and Etzion introduced the concept of Steiner structures in the projective space. In this section, we give its analog in the symplectic space. Also see [12] for Steiner structures in the projective space.

Let $1 \leq \ell \leq m \leq \nu$. A family $\mathcal{F} \subseteq \mathcal{M}(m,0;2\nu)$ is called a *Steiner structure* $S_q[\ell,m;2\nu]$ if the blocks of $\mathcal{F}$ are m-dimensional totally isotropic subspaces, and each ℓ-dimensional subspace in $\mathcal{M}(\ell,0;2\nu)$ is contained in exactly one block from $\mathcal{F}$. Note that trivial Steiner structures $S_q[\ell,\ell;2\nu]$ exist for all $\ell \leq \nu$.

Dye[3] proved the following result: Let $\mathbb{F}_q^{2\nu}$ be the 2ν-dimensional symplectic space. Then there exist ν-dimensional totally isotropic subspaces $V_i,\ i=1,2,\cdots,q^\nu+1$, of $\mathbb{F}_q^{2\nu}$ such that

$$\mathbb{F}_q^{2\nu} = V_1 \cup V_2 \cup \cdots \cup V_{q^\nu+1},$$

where $V_i \cap V_j = \{0\}$ for all $i \neq j$. Note that $\{V_i \mid i = 1,2,\cdots,q^\nu+1\}$ is the Steiner structure $S_q[1,\nu;2\nu]$, which is known as a *ν-symplectic spread* of $\mathbb{F}_q^{2\nu}$.

Lemma 5.1 The total number of blocks in an $S_q[\ell,m;2\nu]$ is $\prod_{t=0}^{l-1}\frac{q^{2(\nu-t)}-1}{q^{m-t}-1}$.

Proof Count pairs $(U,W) \in \mathcal{M}(\ell,0;2\nu)\times\mathcal{M}(m,0;2\nu)$ such that $U \subseteq W$ in two ways. Since each block of $S_q[\ell,m;2\nu]$ contains $\begin{bmatrix} m \\ \ell \end{bmatrix}_q$ ℓ-dimensional subspaces and each ℓ-dimensional subspace in $\mathcal{M}(\ell,0;2\nu)$ is contained in exactly one block, we obtain that the total number of blocks in an $S_q[\ell,m;2\nu]$ is $N(\ell,0;2\nu)/\begin{bmatrix} m \\ \ell \end{bmatrix}_q$ as desired. □

Lemma 5.2 Let $\ell \geq 2$. If $S_q[\ell,m;2\nu]$ exists, then $S_q[\ell-1,m-1;2(\nu-1)]$ exists.

Proof Let $S \subseteq \mathcal{M}(m,0;2\nu)$ be an $S_q[\ell,m;2\nu]$. Pick a fixed one-dimensional subspace $\langle e_1\rangle$. Let

$$S' = \{W \cap \langle e_2,\cdots,e_\nu,e_{\nu+2},\cdots,e_{2\nu}\rangle \mid W \in S, \langle e_1\rangle \subseteq W\}.$$

We show that S' is an $S_q[\ell-1,m-1;2(\nu-1)]$. Note that S' is a set of some $(m-1)$-dimensional totally isotropic subspaces of $\langle e_2,\cdots,e_\nu,e_{\nu+2},\cdots,e_{2\nu}\rangle$. For any $(\ell-1)$-dimensional totally isotropic subspace Y of $\langle e_2,\cdots,e_\nu,e_{\nu+2},\cdots,e_{2\nu}\rangle$, we have that $Y+\langle e_1\rangle$ is an ℓ-dimensional totally isotropic subspace in $\mathcal{M}(m,0;2\nu)$. Hence, $Y+\langle e_1\rangle$ is contained in exactly one block

$W \in S$. Therefore, Y is contained in exactly one element $W \cap \langle e_2, \cdots, e_\nu, e_{\nu+2}, \cdots, e_{2\nu}\rangle$ of S'. Since $\langle e_2, \cdots, e_\nu, e_{\nu+2}, \cdots, e_{2\nu}\rangle$ is isomorphic to $\mathbb{F}_q^{2(\nu-1)}$, S' is an $S_q[\ell-1, m-1; 2(\nu-1)]$. □

Corollary 5.1 If $S_q[\ell, m; 2\nu]$ exists, then $\prod_{t=\nu-\ell+1}^{\nu-i}(q^{2t}-1)/\prod_{t=m-\ell+1}^{m-i}(q^t-1)$ are integers for all $0 \le i \le \ell-1$.

Now we discuss the relations between codes and Steiner structures in the symplectic space.

Theorem 5.1 A Steiner structure $S_q[\ell, m; 2\nu]$ is a $(2\nu, M, 2j, m)$ code with $j = m-\ell+1$ and $M = \prod_{t=0}^{l-1} \frac{q^{2(\nu-t)}-1}{q^{m-t}-1}$.

Proof For any two distinct blocks $U, W \in S_q[\ell, m; 2\nu]$, since every ℓ-dimensional totally isotropic subspace is contained in exactly one block of $S_q[\ell, m; 2\nu]$, we have $\dim(U \cap W) \le \ell - 1$. By (1), we have

$$d(U, W) = 2m - 2\dim(U \cap W) \ge 2(m - \ell + 1),$$

which implies that $j \ge m - \ell + 1$. On the other hand, let V be a fixed $(\ell-1)$-dimensional totally isotropic subspace of $\mathbb{F}_q^{2\nu}$. By the transitivity of $Sp_{2\nu}(\mathbb{F}_q)$ on the set of subspaces of the same type, the number of ℓ-dimensional totally isotropic subspaces of $\mathbb{F}_q^{2\nu}$ containing V is independent of the particular choice of the subspace V. By Lemma 1.5, there are

$$N(\ell-1; \ell-1, 0; \ell, 0; 2\nu) = \frac{q^{2(\nu-\ell+1)}-1}{q-1} \ge 2$$

ℓ-dimensional totally isotropic subspaces of $\mathbb{F}_q^{2\nu}$ containing V, and therefore we can choose two distinct ℓ-dimensional totally isotropic subspaces V_1 and V_2 of $\mathbb{F}_q^{2\nu}$ such that $V = V_1 \cap V_2$. Let U and W be the unique blocks in $S_q[\ell, m; 2\nu]$ such that $V_1 \subseteq U$ and $V_2 \subseteq W$. Then $V = V_1 \cap V_2 \subseteq U \cap W$, which implies $\dim(U \cap W) \ge \dim V = \ell - 1$. Therefore, we have

$$2j \le d(U, W) = 2m - 2\dim(U \cap W) \le 2(m - \ell + 1).$$

Hence $j = m - \ell + 1$ and the desired result follows. □

Theorem 5.2 A $(2\nu, M, 2j, m)$ code $\mathbb{C}$ achieves the Wang-Xing-Safavi-Naini bound, i.e., $M = \prod_{t=0}^{m-j} \frac{q^{2(\nu-t)}-1}{q^{m-t}-1}$, if and only if $\mathbb{C}$ is a Steiner structure $S_q[m-j+1, m; 2\nu]$.

Proof By Theorems 2.2 and 5.1, a Steiner structure $S_q[m-j+1, m; 2\nu]$ is a $(2\nu, M, 2j, m)$ code achieving the Wang-Xing-Safavi-Naini bound. On the other hand, suppose that $\mathbb{C}$ is a $(2\nu, M, 2j, m)$ code achieving the Wang-Xing-Safavi-Naini bound, i.e., $M = \prod_{t=0}^{m-j} \frac{q^{2(\nu-t)}-1}{q^{m-t}-1}$. Since the distance between any two different codewords of $\mathbb{C}$ is not small than $2j$, by (1) each $(m-j+1)$-dimensional totally isotropic subspace of $\mathbb{F}_q^{2\nu}$ cannot be contained in two distinct codewords. Since each codeword of $\mathbb{C}$ contains $\begin{bmatrix} m \\ m-j+1 \end{bmatrix}_q$ $(m-j+1)$-dimensional totally isotropic subspaces, all codewords of $\mathbb{C}$ contains

$$M \begin{bmatrix} m \\ m-j+1 \end{bmatrix}_q = N(m-j+1, 0; 2\nu)$$

distinct $(m-j+1)$-dimensional totally isotropic subspaces, which implies that each $(m-j+1)$-dimensional totally isotropic subspace is contained in exactly one codeword of $\mathbb{C}$. Therefore, regarding the codewords of $\mathbb{C}$ as blocks, $\mathbb{C}$ forms a Steiner structure $S_q[m-j+1, m; 2\nu]$. □

Remark 5.1 A *t-spread* of the vector space $\mathbb{F}_q^m$ is a set $\mathcal{P}$ of t-dimensional subspaces of $\mathbb{F}_q^m$ such that any non-zero vector is contained in exactly one element of $\mathcal{P}$. It is well known that a t-spread of $\mathbb{F}_q^m$ exists if and only if t is a divisor of m, see [2]. Let $\mathbb{F}_q^{2\nu}$ be the 2ν-dimensional symplectic space, and $\{V_i \mid i = 1, 2, \cdots, q^\nu + 1\}$ be a symplectic spread of $\mathbb{F}_q^{2\nu}$. Suppose $\nu = tk$ with $2 \le t \le \nu - 1$. Let $\mathcal{P}_i$ be a t-spread of V_i for $i = 1, 2, \cdots, q^\nu + 1$. Then $\bigcup_{i=1}^{q^\nu+1} \mathcal{P}_i$ is the Steiner structure $S_q[1, t; 2\nu]$. In particular, the Steiner structure $S_q[1, 2; 8]$ exists.

Theorem 5.2 tells us that Steiner structures are optimal codes. By Theorem 5.2 we obtain the following corollary.

Corollary 5.2 $\mathcal{A}(2\nu, 2j, m) = \prod_{t=0}^{m-j} \frac{q^{2(\nu-t)}-1}{q^{m-t}-1}$ if and only if a Steiner structure $S_q[m - j + 1, m; 2\nu]$ exists.

6 The Bounds on the Size of Codes in $\mathcal{M}(2\nu)$

Let $\mathcal{A}(2\nu, d)$ denote the maximum number of codewords in a $(2\nu, M, d)$ code in $\mathcal{M}(2\nu)$. In this section, we study the upper and lower bounds on $\mathcal{A}(2\nu, d)$.

The *sphere* of radius r centered at a subspace U in $\mathcal{M}(2\nu)$ is defined to be the set of all subspaces whose distance from U is less than or equal to r, i.e., the set

$$S_r(U) = \{W \in \mathcal{M}(2\nu) \mid d(U, W) \le r\}.$$

Lemma 6.1 Let $U \in \mathcal{M}(\ell, 0; 2\nu)$. Then

$$|S_r(U)| = \sum_{k=0}^{\nu} \sum_{t=\lceil(\ell+k-r)/2\rceil}^{\min\{\ell,k\}} N(t; \ell, 0; k, 0; 2\nu).$$

Proof For any $W \in S_r(U) \cap \mathcal{M}(k, 0; 2\nu)$, by (1) $d(U, W) \le r$ if and only if $\ell + k - 2\dim(U \cap W) \le r$, which implies that $\dim(U \cap W) \ge \lceil \frac{\ell+k-r}{2} \rceil$. By Lemma 1.5, one obtains that

$$|S_r(U) \cap \mathcal{M}(k, 0; 2\nu)| = \sum_{t=\lceil(\ell+k-r)/2\rceil}^{\min\{\ell,k\}} N(t; \ell, 0; k, 0; 2\nu).$$

It follows that

$$|S_r(U)| = \sum_{k=0}^{\nu} |S_r(U) \cap \mathcal{M}(k, 0; 2\nu)| = \sum_{k=0}^{\nu} \sum_{t=\lceil(\ell+k-r)/2\rceil}^{\min\{\ell,k\}} N(t; \ell, 0; k, 0; 2\nu)$$

as desired. □

By the transitivity of $Sp_{2\nu}(\mathbb{F}_q)$ on the set of subspaces of the same type, the size of $S_r(U)$ in Lemma 6.1 is independent of the particular choice of the subspace U. Therefore, we can write $S_r^\ell = |S_r(U)|$ for each $U \in \mathcal{M}(\ell, 0; 2\nu)$.

Tolhuizen[13] obtained the following result: if $\widetilde{S}_r$ is the average size of a sphere of radius r in a graph $G = (V, E)$, then there exists a code $\mathbb{C}$ in G with minimum (graph) distance d and $|\mathbb{C}| \ge |V|/\widetilde{S}_{d-1}$. By using Tolhuizen's result, we obtain the Gilbert-Varshamov bound on the size of codes in $\mathcal{M}(2\nu)$.

Theorem 6.1 (Gilbert-Varshamov bound)

$$\mathcal{A}(2\nu, d) \ge \frac{\sum_{\ell=0}^{\nu} \sum_{k=0}^{\nu} {\nu \brack \ell}_q {\nu \brack k}_q \prod_{t=\nu-\ell+1}^{\nu} (q^t + 1) \prod_{t=\nu-k+1}^{\nu} (q^t + 1)}{\sum_{\ell=0}^{\nu} \sum_{k=0}^{\nu} \sum_{t=\lceil(\ell+k-d+1)/2\rceil}^{\min\{\ell,k\}} {\nu \brack \ell}_q \prod_{t=\nu-\ell+1}^{\nu} (q^t + 1) N(t; \ell, 0; k, 0; 2\nu)}.$$

Proof Let Γ be the graph with the vertex set $\mathcal{M}(2\nu)$. Then

$$\widetilde{S}_{d-1}=\frac{\sum_{U\in\mathcal{M}(2\nu)}|S_{d-1}(U)|}{|\mathcal{M}(2\nu)|}=\frac{\sum_{\ell=0}^{\nu}|\mathcal{M}(\ell,0;2\nu)|S_{d-1}^{\ell}}{|\mathcal{M}(2\nu)|}$$

is the average size of a sphere of radius $d-1$ in Γ. By Lemma 6.1 we have

$$\mathcal{A}(2\nu,d)\geq\frac{|\mathcal{M}(2\nu)|}{\widetilde{S}_{d-1}}=\frac{|\mathcal{M}(2\nu)|^2}{\sum_{\ell=0}^{\nu}|\mathcal{M}(\ell,0;2\nu)|S_{d-1}^{\ell}}$$

as desired. □

Given a code $\mathbb{C}$ in $\mathcal{M}(2\nu)$, let $D_0,D_1,\cdots,D_\nu$ denote its *dimension distribution*. That is, $D_k=|\mathbb{C}\cap\mathcal{M}(k,0;2\nu)|$ for $k=0,1,\cdots,\nu$. Set $D_k=0$ for $k\notin\{0,1,\cdots,\nu\}$. The following theorem employs linear programming to establish an upper bound on $\mathcal{A}(2\nu,d)$.

Theorem 6.2 Let $D_0,D_1,\cdots,D_\nu$ denote the dimension distribution of a $(2\nu,M,2e+1)$ code $\mathbb{C}$ in $\mathcal{M}(2\nu)$. Let $f^*=\max\sum_{m=0}^{\nu}D_m$, subject to the $2\nu+2$ linear constrains

$$D_m\leq\mathcal{A}(2\nu,2e+2,m)\quad\text{for } m=0,1,\cdots,\nu,$$
$$\sum_{\ell=0}^{\nu}\sum_{t=\lceil(\ell+m-e)/2\rceil}^{\min\{\ell,m\}}N(t;\ell,0;m,0;2\nu)D_\ell\leq N(m,0;2\nu)\quad\text{for } m=0,1,\cdots,\nu.$$

Then f^* is an upper bound on $\mathcal{A}(2\nu,2e+1)$.

Proof Since the distance between any two elements of $\mathbb{C}\cap\mathcal{M}(m,0;2\nu)$ is always even, $D_m=|\mathbb{C}\cap\mathcal{M}(m,0;2\nu)|\leq\mathcal{A}(2\nu,2e+2,m)$ for $m=0,1,\cdots,\nu$. Note that spheres of radius e about the codewords of $\mathbb{C}$ are disjoint. Now we count the number of m-dimensional totally isotropic subspaces contained in such spheres. For each $U\in\mathbb{C}\cap\mathcal{M}(\ell,0;2\nu)$, by Lemma 1.5 there are

$$\sum_{t=\lceil(\ell+m-e)/2\rceil}^{\min\{\ell,m\}}N(t;\ell,0;m,0;2\nu)$$

distinct m-dimensional totally isotropic subspaces contained in the sphere of radius e centered at U, which implies that

$$\sum_{\ell=0}^{\nu}\sum_{t=\lceil(\ell+m-e)/2\rceil}^{\min\{\ell,m\}}N(t;\ell,0;m,0;2\nu)D_\ell\leq N(m,0;2\nu)$$

for $m=0,1,\cdots,\nu$. □

Remark 6.1 Let $\nu=2$. By Theorem 6.2 we obtain $f^*=2(q^3+q^2+q)+3$ if $e=0$, and $f^*=q^2+1$ if $e=1$. Note that a $(4,2(q^3+q^2+q)+3,1)$ code in $\mathcal{M}(4)$ is the set of all totally isotropic subspaces of the symplectic space $\mathbb{F}_q^4$, and a $(4,q^2+1,3)$ code in $\mathcal{M}(4)$ is a 2-symplectic spread of the symplectic space $\mathbb{F}_q^4$.

Remark 6.2 (1) Let $\mathbb{F}_q^{2\nu}$ be the 2ν-dimensional symplectic space and P_0 be a fixed ν-dimensional totally isotropic subspace of $\mathbb{F}_q^{2\nu}$. Then $\mathcal{M}(0;\nu,0;m,0;2\nu)\subseteq\mathcal{M}(m,0;2\nu)$. Note that codes in $\mathcal{M}(0;\nu,0;m,0;2\nu)$ are subcodes of some codes in $\mathcal{M}(m,0;2\nu)$. It seems to be interesting to discuss the codes in $\mathcal{M}(0;\nu,0;m,0;2\nu)$.

(2) Let $\mathbb{F}_q^n$ be one of the n-dimensional classical spaces and G_n be the corresponding classical group. This article studies the codes of $\mathbb{F}_q^n$ when G_n is the symplectic group. It seems to be interesting to discuss the codes of $\mathbb{F}_q^n$ when G_n is the unitary and orthogonal groups.

Acknowledgements We would like to thank the referees for their valuable suggestions.

References

[1] Ahlswede, R. and Aydinian, H., On error control codes for random network coding, IEEE Workshop on Network Coding, Theory and Applications, 2009, 68-73.

[2] Dembowski, P., Finite Geometries, Berlin: Springer-Verlag, 1968.

[3] Dye, R.H., Partitions and their stabilizers for line complexes and quadrics, *Ann. Mat. Pura Appl.*, 1977, 114: 173-194.

[4] Etzion, T. and Vardy, A., Error-correcting codes in projective spaces, *IEEE Trans. Inf. Theory*, 2011, 57: 1165-1173.

[5] Gao, Y. and Wang, G., Error-correcting codes in attenuated space over finite fields, *Finite Fields Appl.*, 2015, 33: 103-117.

[6] Guo, J., Li, F. and Wang, K., Anzahl formulas of subspaces in symplectic spaces and their applications, *Linear Algebra Appl.*, 2013, 438: 3321-3335.

[7] Guo, J., Ma, J. and Wang, K., Erdős-Ko-Rado theorems in certain semilattices, *Sci. China Math.*, 2013, 56: 2393-2407.

[8] Huffman, W.C. and Pless. V., Fundamentals of Error-correcting Codes, Cambridge: Cambridge Univ. Press, 2003.

[9] Kötter, R. and Kschischang, F.R., Coding for errors and erasures in random network coding, *IEEE Trans. Inf. Theory*, 2008, 54: 3579-3591.

[10] MacWilliams, F.J. and Sloane, N.J.A., The Theory of Error-correcting Codes, Amsterdam: North-Holland, 1977.

[11] Schwartz, M. and Etzion, T., Codes and anticodes in the Grassmann graph, *J. Combin. Theory Ser. A*, 2002, 97: 27-42.

[12] Thomas, S., Designs over finite fields, *Geometriae Dedicata*, 1987, 21: 237-242.

[13] Tolhuizen, L.M.G., The generalized Gilbert-Varshamov bound is implied by Turán theorem, *IEEE Trans. Inf. Theory*, 1997, 43: 1605-1606.

[14] Wan, Z., Geometry of Classical Groups Over Finite Fields, 2nd Edition, Beijing: Science Press, 2002.

[15] Wang, H., Xing, C. and Safavi-Naini, R.M., Linear authentication codes: bounds and constructions, *IEEE Trans. Inf. Theory*, 2003, 49: 866-872.

[16] Xia, S.T. and Fu, F.W., Johnson type bounds on constant dimension codes, *Des. Codes Cryptogr.*, 2009, 50: 163-172.

基于辛空间中全迷向子空间的纠错码

郭　军[1]，李凤高[2]

(1. 廊坊师范学院数学与信息科学学院，廊坊，河北，065000； 2. 湖南理工学院数学学院，岳阳，湖南，414006)

摘要： 设 $\mathbb{F}_q^{2\nu}$ 是 q 元有限域 $\mathbb{F}_q$ 上的 2ν 维辛空间. 对于给定的整数 $0 \le m \le \nu$, 设 $\mathcal{M}(m,0;2\nu)$ 是 $\mathbb{F}_q^{2\nu}$ 的所有 m 维全迷向子空间的集合, 而 $\mathcal{M}(2\nu)=\bigcup_{m=0}^{\nu}\mathcal{M}(m,0;2\nu)$. 本文给出了 $\mathcal{M}(2\nu)$ 中码的大小的界, 并且证明了在给出 $\mathcal{M}(m,0;2\nu)$ 中的码达到 Wang-Xing-Safavi-Naini 界当且仅当它是某个 Steiner 结构.

关键词： 纠错码; 辛空间; 全迷向子空间; Steiner 结构